UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

In re:
Eureka Casino Breach Litigation

Case No. 2:23-cv-00276-CDS-BNW

Order Granting in Part and Denying in Part Defendant's Motion to Dismiss

[ECF No. 41]

Plaintiffs William Houghton, Andrew Figura, Michael Oldham, and Kristin Andrew,[1] individually and on behalf of all others similarly situated, bring this action against Defendant Rancho Mesquite Casino, Inc. d/b/a Eureka Casino Hotel ("Eureka"). Am. Compl., ECF No. 31. Collectively, they assert claims for: (1) negligence; (2) negligence per se; (3) breach of implied contract; (4) unjust enrichment; (5) violation of the California Unfair Competition Law ("UCL"); (6) violation of the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100, et seq.) ("CCPA"); (7) violation of the California Customer Records Act (Cal. Civ. Code §§ 1798.80, et seq.) ("CCRA"); and (8) declaratory judgment. *Id.* Eureka filed a motion to dismiss, ECF No. 41, which has been fully briefed.[2] For the reasons set forth herein, I grant in part and deny in part the motion to dismiss.

I. Background[3]

Defendant Eureka owns and operates hotels and casinos in Mesquite, Nevada, Las Vegas, Nevada, and Seabrook, New Hampshire. ECF No. 31 at ¶ 26. From around November 9, 2022, to November 13, 2022, Eureka was subject to a data breach which reportedly involved the personal information of at least 229,299 individuals, many of whom were Eureka customers. *Id.* at ¶ 1. The

[1] Hereinafter referred to collectively as the "Houghton plaintiffs."
[2] Opp'n to the Eureka's mot. to dismiss, ECF No. 42; Reply to the mot. to dismiss, ECF No. 43.
[3] Unless otherwise noted as undisputed, references to the consolidated complaint in this section are for background information only and do not serve as findings of fact.

Houghton plaintiffs allege that "cybercriminals gained unauthorized access to [Eureka]'s computer systems and networks and acquired copies of Private Information held on [Eureka]'s systems" and Eureka "only became aware of the unauthorized access when the cyberthieves encrypted [Eureka]'s computer systems as part of a ransomware attack." *Id.* at ¶¶ 32–33.

Information involved in the data breach included, but was not necessarily limited to, individuals' full names, Social Security numbers, and driver's license numbers. *Id.* at ¶ 2. The Houghton plaintiffs allege that they are current or former customers of Eureka. *Id.* at ¶¶ 102, 108, 114, 120. Plaintiffs Houghton, Oldham, and Andrew are or were members of Eureka's players rewards club. *Id.* ¶¶ 102, 108, 114. Each provided Eureka with their name, Social Security number, "and other Private Information" in exchange for payment and for membership in its players club. *Id.* Plaintiff Figura was a customer of Eureka and alleges that he was required to supply Eureka "with his name and other Private Information as a condition of using [Eureka]'s services and facilities." *Id.* at ¶ 120.

Each of the Houghton plaintiffs received a letter from Eureka on February 16, 2023, explaining that, on November 9, 2022, Eureka had "experienced a cybersecurity incident in which some of [its] systems were encrypted by an unauthorized actor."[4] *Id.* at ¶¶ 31–36. They allege that Eureka "failed to encrypt the [Personally Identifiable Information ("PII")] stored on its computer systems, evidenced by the fact that hackers were able to steal the Private Information in a readable form." *Id.* at ¶ 38. The Houghton plaintiffs cite to a notice by Eureka announcing the breach, which stated that "[u]pon discovering the incident, we immediately took steps to secure our system[,]" and recommended that affected individuals "remain vigilant by reviewing your credit reports and account statements for any unauthorized activity." *Id.* at ¶¶ 39–40 (citing Office of the Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/35af8dca-9af6-4a5d-aa9b-

[4] The Houghton plaintiffs allege 1,737 of the impacted individuals received notice earlier, on December 9, 2022. *Id.* at ¶ 36.

d7013c99d9d6.shtml).

Between February 22 and March 16, 2023, the four Houghton plaintiffs filed individual complaints in this court asserting claims against Eureka arising out of the cyberattack. ECF No. 6; ECF No. 27. On June 16, 2023, following entry of an order of consolidation, the Houghton plaintiffs filed a consolidated class action complaint on behalf of themselves, a putative nationwide class, and a California sub-class comprised of others who are similarly situated. ECF No. 31. Eureka filed a motion to dismiss all eight of the Houghton plaintiffs' claims on September 15, 2023. ECF No. 41.

II. Legal standard

The Federal Rules of Civil Procedure require a plaintiff to plead "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Dismissal is appropriate under Rule 12(b)(6) when a pleader fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A pleading must give fair notice of a legally cognizable claim and the grounds on which it rests, and although a court must take all factual allegations as true, legal conclusions couched as factual allegations are insufficient. *Twombly*, 550 U.S. at 555. Accordingly, Rule 12(b)(6) requires "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* This standard "asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*

If the court grants a motion to dismiss for failure to state a claim, leave to amend should be granted unless it is clear that the deficiencies of the complaint cannot be cured by amendment. *DeSoto v. Yellow Freight Sys., Inc.*, 957 F.2d 655, 658 (9th Cir. 1992). Under Rule 15(a), a

court should "freely" give leave to amend "when justice so requires," and in the absence of a reason such as "undue delay, bad faith or dilatory motive of the part of the movant, repeated failure to cure deficiencies by amendment previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, futility of the amendment, etc." *Foman v. Davis*, 371 U.S. 178 (1962).

III. Discussion

Defendant Eureka moves to dismiss all of plaintiffs' common law and statutory claims. The court addresses plaintiffs' claims in turn.

A. Cognizable damages for negligence and breach of implied contract claims

A "plaintiff must prove damages to prevail on" negligence[5] and breach of implied contract claims. *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1231–32 (D. Nev. 2020), *aff'd*, 845 F. App'x 613 (9th Cir. 2021) (citing *Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc.*, 221 P.3d 1276, 1280 (Nev. 2009), and *Saini v. Int'l Game Tech.*, 434 F. Supp. 2d 913, 919–20 (D. Nev. 2006)) (*Pruchnicki I*). To prove damages, a plaintiff must have a cognizable injury that is not "too tenuous[.]" *Id.* at 1232. *See also Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010) (finding that allegations of certain future harm was too tenuous to support a cognizable injury in a negligence claim). The Houghton plaintiffs assert several cognizable injuries to support damages in their negligence and breach of contract claims, all of which Eureka disputes.

1. Loss of time

In their consolidated complaint, the Houghton plaintiffs state that they have suffered damages for "loss of time" needed to "take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach." ECF No. 31 at ¶ 14.

[5] Because the Houghton plaintiffs withdraw their cause of action for negligence per se, I will not address it further. *See* ECF No. 42 at 2 n.2.

Eureka argues that the time lost to protecting information is "an unfortunate, but common, fact of daily life in a digital world[,]" arguing that there is no way to make lost time damages cognizable absent tangible, out-of-pocket expenses. ECF No. 43 at 5 (citing *Pruchnicki I*, 439 F. Supp. 3d at 1233 and *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 134 (D. Me. 2009), *aff'd in part, rev'd in part sub nom. on other grounds*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 156 (1st Cir. 2011)).

The Houghton plaintiffs do not allege any additional out-of-pocket expenses they made in protecting their data. *See* ECF No. 31 at ¶ 14. "[L]ost time alone does not establish compensable damages." *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1192 (D. Nev. 2022) (citing *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613, 614 (9th Cir. 2021) (*Prucknicki II*)). Unlike out-of-pocket expenses incurred in protecting one's data and responding to a data breach, which provide a concrete measure of a plaintiff's damages, a claim for lost time by itself is simply too nebulous. Accordingly, I dismiss the Houghton plaintiffs' negligence claim to the extent it alleges damages based on loss of time. However, because it is unclear if amendment could cure this deficiency, dismissal is without prejudice and with leave to amend.

2. Emotional distress

The Houghton plaintiffs allege they suffered emotional distress because of the data breach. ECF No. 31 at ¶¶ 105, 111, 117, 135. Arguing for dismissal, Eureka cites *Pruchnicki I*, which states that "Nevada law 'require[s] a plaintiff to demonstrate that he or she has suffered some physical manifestation of emotional distress in order to support an award of emotional damages.'" *Pruchnicki I*, 439 F. Supp. at 1233 (quoting *Betsinger v. D.R. Horton, Inc.*, 232 P.3d 433, 436 (Nev. 2010)). *See also Pruchnicki II*, 845 F. App'x at 614 ("[U]nder Nevada law, 'in the absence of physical impact, proof of "serious emotional distress" causing physical injury or illness must be presented.'" (quoting *Olivero v. Lowe*, 995 P.2d 1023, 1026 (Nev. 2000)). Houghton, Oldham, and Andrew allege that their emotion distress has manifested as "anxiety about unauthorized parties viewing, selling, and/or using [their] Private Information for purposes of identity theft and fraud.

[They are] very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach." ECF No. 31 at ¶¶ 105, 111, 117. None of this can be characterized as physical injury or even "serious" emotional distress. *Pruchnicki II*, 845 F. App'x at 614. Accordingly, I dismiss without prejudice, and with leave to amend, the Houghton plaintiffs' negligence claim to the extent it alleges damages based on emotional distress.

3. Violation of privacy

The Houghton plaintiffs seemingly argue "violation of privacy" as a cognizable harm that arises out of the data breach. ECF No. 31 at ¶¶ 106, 112, 118, 123, 133, 135. Eureka argues that the Houghton plaintiffs fail to address how such a violation resulted in compensable damages, citing several cases, including *Aguilar v. Hartford Accident & Indem. Co.* ECF No. 41 at 12. In *Aguilar*, the court held that "the loss of privacy engendered by an accidental data breach cannot satisfy the necessary damage element of a negligence claim, 'without specific factual statements that Plaintiffs' Personal Information has been misused, in the form of an open bank account, or un-reimbursed charges.'" 2019 WL 2912861, at *2 (C.D. Cal. Mar. 13, 2019) (quoting *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012)). In opposition, the Houghton plaintiffs rely primarily on a case that addresses violation of privacy for purposes of Article III standing as opposed to damages. ECF No. 42 at 17 (citing *Medoff v. Minka Lighting, LLC*, 2023 WL 4291973, at *3 (C.D. Cal. May 8, 2023)).[6] They also cite *Smallman*, which states that "[i]n the data breach context, courts within the Ninth Circuit have found that an individual's loss of control over the use of their identity due to a data breach and the

[6] The question of whether a plaintiff has alleged sufficient injury for standing purposes is a separate inquiry from whether they have stated a claim for compensable damages, and their having adequately pled one does not automatically mean they have sufficiently pled both. *See Pruchnicki II*, 845 F. App'x at 614–15 (finding that the district court in *Pruchnicki I* acted within its discretion when it found that the plaintiff sufficiently alleged injury for standing purposes but did not state a claim for compensable damages). Eureka did not challenge the Houghton plaintiffs' standing to bring this claim for relief.

accompanying impairment in value of PII constitutes non-economic harms." 638 F. Supp. 3d at 1188.

It appears the Houghton plaintiffs' theory of damages as to this claim is an evolving one. What was pled as a "violation" of privacy in their consolidated complaint transformed into an "invasion" of their privacy rights and, supported by a citation to *Smallman*, a violation of their "right to control" their PII in their opposition to Eureka's motion. *Compare* ECF No. 31 at ¶¶ 106, 112, 118, 123, 133, 135 ("violation"), *with* ECF No. 42 at 17 ("invasion" and "right to control"). The plaintiffs do not explain the reasoning behind their violations of privacy claims in their consolidated complaint and provide confusing citations to other bases of harm in their opposition. The plaintiffs' allegations regarding a "violation of privacy" are not pled with sufficient specificity to survive a Rule 12(b)(6) motion to dismiss. Therefore, I dismiss without prejudice, and with leave to amend, the Houghton plaintiffs' negligence claim to the extent it alleges damages based on a violation of privacy.

4. Increased/future risk of identity theft

The Houghton plaintiffs allege that they face an increased risk of being "targeted in the future, subjected to phishing, data intrusion, and other illegal actions based on their Private Information as potential fraudsters could use that information to target such schemes more effectively." ECF No. 31 at ¶ 126. In its motion, Eureka argues that the plaintiffs' claim is too speculative, and "mere risk of future harm does not constitute cognizable injury." ECF No. 41 at 6. It cites to *Pruchnicki I*, in which the court held that "alleged injuries that stem from the danger of future harm are insufficient to support a negligence action." 439 F. Supp. 3d at 1232 (citing *Krottner*, 406 F. App'x at 131). The *Pruchnicki I* court held that "the imminent and certainly impending injury flowing from potential fraud and identity theft and the continued risk to [the plaintiff's] personal data are too tenuous to constitute damages as an element of plaintiff's

claim." *Id.* at 1232 (internal quotations omitted).[7] In their opposition, the Houghton plaintiffs respond by citing to *Smallman*, in which the court held

> that the rightful determination is "not to look at the minutia of what information has been taken — such as credit card information — or social security numbers — but to specifically determine whether the data taken 'gave hackers the means to commit fraud or identity theft.'" *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1034 (N.D. Cal. 2019) (quoting [*In re Zappos.com, Inc.*, 888 F.3d 1020, 1027–29 (9th Cir. 2018)]. "The information taken . . . need not be sensitive to weaponize hackers in their quest to commit further fraud or identity theft." *Bass*, 394 F. Supp. 3d at 1034. "Imminent injury in fact can be established through information similar in function to [a] social security number[ ]," which "derives its value in that it is immutable." *Id.*

Smallman, 638 F. Supp. 3d at 1191. It is important to note that the *Smallman* case presented a very different set of factual allegations. Unlike here, the *Smallman* plaintiffs specifically alleged that they already had their hacked information "posted for sale on the dark web" and multiple plaintiffs claimed that "criminals ha[d] attempted to make fraudulent purchases on their accounts." *Id.* However, *Smallman* also notes a Seventh Circuit opinion that acknowledged: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.* at 1191–92 (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)).[8]

The Ninth Circuit cases on which both *Pruchnicki I* and *Smallman* rely—*Krottner* and *In re Zappos*, respectively—address issues of standing, not cognizable harm for purposes of damages. *See Krottner*, 628 F.3d at 1142; *In re Zappos*, 888 F.3d at 1024. There does not appear to be any clear guidance in the Ninth Circuit as to whether, and to what extent, future risk of harm can serve as

---

[7] Aside from stating that Nevada law does not permit recovery of speculative damages, the Ninth Circuit in *Pruchnicki II* did not address the district court's finding on this issue of increased or future risk of identity theft. *See Pruchnicki II*, 845 F. App'x at 614–15.

[8] *Smallman* also cites to a Sixth Circuit opinion which held that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." *Smallman*, 638 F. Supp. 3d at 1192 (quoting *Galaria v. Nationwide Mut. Ins. Co.*, 663 F App'x 384, 388 (6th Cir. 2016)). I also agree with this reasoning set forth in *Galaria*.

a cognizable injury. But I find the Seventh Circuit's reasoning in *Remijas* persuasive: regardless of whether a plaintiff alleges their hacked information has been shared or sold, the purpose of a hack is to collect and then utilize the plaintiffs' private information to make fraudulent charges, take their identities, or sell to others who will do either or both. Plaintiffs do not have to wait until hackers inevitably use their private information for nefarious purposes to allege a cognizable injury. Therefore, I deny Eureka's motion to the extent it seeks dismissal on the grounds that the plaintiffs' allegation of future risk of injury is not a cognizable harm.

5. Diminution in value

The Houghton plaintiffs allege that they suffered cognizable harm because the hack of their PII has diminished its value. ECF No. 31 ¶¶ 106, 112, 117, 123. "Diminution in value of personal information can be a viable theory of damages." *Pruchnicki I*, 439 F. Supp. 3d at 1234. In its motion to dismiss, Eureka argues that a plaintiff may sufficiently allege diminution in value of personal information as a cognizable injury only when they have plausibly alleged: (1) the "existence of a market for [their] personal information" and (2) "an impairment of [their] ability to participate in that market." ECF No. 41 at 8 (quoting *Svenson v. Google Inc.*, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016), and citing *Pruchnicki I*, 439 F. Supp. 3d at 1234). It argues that "[t]he only market for the sale of these types of personal information is the criminal underground." *Id.* (citing *Griffey v. Magellan Health, Inc.*, 562 F. Supp. 3d 34, 46 (D. Ariz. 2021), and *Pruchnicki I*, 439 F. Supp. 3d at 1234, for the proposition that a diminution of value theory only applies to items or information for which there are lawful markets). Eureka also argues that the Houghton plaintiffs "have not alleged that they have been impaired from participating in any legitimate market in which they could sell or monetize their Social Security or driver's license numbers." *Id.*

In their opposition, the Houghton plaintiffs again point to *Smallman*, in which the court, rather than evaluating the market value of the plaintiffs' PII, held that "[a]ny past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace." ECF No. 42 at 14 (quoting *Smallman*, 638 F. Supp. 3d at 1191). The plaintiffs also cite to a

"growing trend" among courts to "recognize 'the value of consumer personal information is not derived solely (or even realistically) by its worth in some imagined marketplace where the consumer actually seeks to sell it to the highest bidder, but rather in the economic benefit the consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check.'" *Id.* (quoting *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020), and citing *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1204 (S.D. Fla. 2022)). The plaintiffs argue that, in the increasingly digital world, a plaintiff "need not allege that they intended to sell their PII because PII derives its value to consumers by enabling them to participate in ordinary life and they are entitled to damages resulting from the diminished value of their PII." *Id.* (citing *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) (*Anthem I*)).

Eureka's interpretation of diminution in value is too narrow. *See Smallman*, 638 F. Supp. 3d at 1190 ("[The] pleading requirements, that Plaintiffs must establish both the existence of a market for their PII and an impairment of their ability to participate in that market, is not supported by Ninth Circuit precedent and other district courts in this Circuit have rejected them."); *Anthem I*, 2016 WL 3029783, at *15 ("These statements [in the case law] appear to require a plaintiff to allege that there was either an economic market for their PII or that it would be harder to sell their own PII, not both."). The value of personal information in the digital world is fundamentally different from what might be considered a loss of value in a "typical" market. The "Data Breach devalued Plaintiffs' PII by interfering with their fiscal autonomy. "Any . . . potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace." *Smallman*, 638 F. Supp. 3d at 1191. Therefore, I deny Eureka's motion to the extent it seeks dismissal on the grounds that the plaintiffs' allegation of diminution of value of their PII is not a cognizable harm.

6. Benefit of the bargain

The Houghton plaintiffs allege that they "lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration." ECF No. 31 at ¶ 65. To support their allegations, they state that "they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiffs' and Class Members' Private Information." *Id.* at 27. And "[h]ad Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased services and/or products from Defendant." *Id.* at 37.

In seeking dismissal, Eureka argues that, as a matter of law, the plaintiffs "could not have bargained for 'reasonable data security' because Defendant had a pre-existing duty to provide such[,]" and California and Nevada laws require a business to maintain reasonable security measures for peoples' PII. ECF No. 41 at 9 (citing NRS 603A.210 and Cal. Civ. Code § 1798.81.5). Additionally, it argues that the Houghton plaintiffs do not allege that they were denied "any gambling, lodging, food and beverage, or club membership services for which they supplied personal information" or that Eureka "made any 'affirmative representation that data security was included in the cost of the goods [or services that Plaintiffs' allegedly purchased from Defendant].'" *Id.* (quoting *Gardiner v. Walmart, Inc.*, 2021 WL 4992539, at *5 (N.D. Cal. July 28, 2021) (alterations in motion). In response, the Houghton plaintiffs argue that they "paid money and provided their PII to Eureka in exchange for its services, inherent to which was the mutual understanding that Eureka would safeguard that PII[,]" and "the promise to safeguard PII is implicit to every exchange involving confidential information." ECF No. 42 at 15 (citing *Smallman*, 638 F. Supp. 3d at 1190).

First, the existence of rules requiring reasonable security measures do not inherently negate a claim for benefit-of-bargain damages. *See, e.g.*, *Smallman*, 638 F. Supp. 3d at 1190. Even the case upon which Eureka relies, *In re Banner Health Data Breach Litig.*, supports this point. *See* 2018 WL 11352137 at *2–3 (D. Ariz. Aug. 7, 2018) (holding that, in the case of medical information, "when promising to protect the data of Patient and Insurance Plan Plaintiffs, Defendant would have needed to promise to do more than merely comply with the HIPAA for the agreement to be enforceable" but "courts may presume that a party who provides sensitive information while receiving a job, a good, or a service may expect that the information is reasonably protected").

Although Eureka describes the plaintiffs' theory as "newfangled," ECF No. 43 at 5, a significant body of case law supports it is a cognizable harm. Indeed, the district court in *Smallman* summarized the current state of Ninth Circuit case law. It first described a series of cases in which courts have accepted "more general allegations that data security was expected and was part of the bargain" and then another line of cases in which "required more specific factual allegations showing how data security was a part of the bargain or how much of the money spent was for data security." *Smallman*, 638 F. Supp. 3d at 1189–90 (collecting cases). The *Smallman* court was persuaded by the first line of cases, reasoning that the second line required plaintiffs to allege more than is necessary to survive a motion to dismiss. *Id.* at 1190. I too am persuaded by this reasoning. It is sufficient for a plaintiff to allege that their overpayment for services came with the expectation that they would be conferred the benefit of adequate data security, and that, had they known that the defendant's security measures were less than industry-standard, they would not have gone through with their transaction. Therefore, I deny Eureka's motion to the extent it seeks dismissal on the grounds that the plaintiffs' allegation that they lost the benefit of their bargain for data security is not a cognizable harm.

B. Economic loss doctrine

In its motion, Eureka argues that the Houghton plaintiffs' negligence claim is barred under the economic loss doctrine. ECF No. 41 at 12. The economic loss doctrine "generally 'bars

unintentional tort actions when the plaintiff seeks to recover purely economic losses.'" *Lombino v. Bank of Am., N.A.*, 797 F. Supp. 2d 1078, 1082 (D. Nev. 2011) (quoting *Terracon Consultants W., Inc. v. Mandalay Resort Grp.*, 206 P.3d 81, 86 (Nev. 2009)). "Thus, the doctrine provides that certain economic losses are properly remediable only in contract." *Peri & Sons Farms, Inc. v. Jain Irr., Inc.*, 933 F. Supp. 2d 1279, 1283–84 (D. Nev. 2013). Nevada defines the economic loss doctrine as "the loss of the benefit of the user's bargain including pecuniary damage for all inadequate value, the cost of repair and replacement of the defective product, or consequent loss of profits, without any claim of personal injury or damage to other property." *Id.* (citation omitted). Therefore, the economic loss doctrine "does not bar actions seeking damage for pecuniary losses that are 'accompan[ied by] personal injury or property damage.'" *Id.* (quoting *Terracon*, 206 P.3d at 86).

Courts in the Ninth Circuit have consistently found that the loss of control of a plaintiff's identity and the resulting impairment of value of the PII in data breach cases constitutes non-economic harm. *See Smallman*, 638 F. Supp. 3d at 1188; *Flores-Mendez v. Zoosk, Inc.*, 2021 WL 308543, at *3 (N.D. Cal. Jan. 30, 2021) (finding that the plaintiffs' allegation of an enlarged risk of identity theft, among others, prevented the dismissal of the negligence claim based on the economic loss doctrine). Here, because the Houghton plaintiffs have sufficiently alleged harm under a theory of increased risk of identity theft, the harms are not purely economic. Therefore, I deny Eureka's motion to the extent it seeks dismissal on the grounds that the plaintiffs' negligence claim is barred by the economic loss doctrine. The Houghton plaintiffs have sufficiently pled a claim for negligence against Eureka.

C. Implied contract

Nevada law requires the plaintiff in a breach of contract action to show: (1) the existence of a valid contract; (2) a breach by the defendant; and (3) damage as a result of the breach. *Mizrahi v. Wells Fargo Home Mortg.*, 2010 WL 2521742, at *3 (D. Nev. June 16, 2010) (citing *Saini*, 434 F. Supp. 2d at 919–20). Although the terms of an implied contract are manifested by conduct rather than written words, both "are founded upon an ascertainable agreement." *Smith v. Recrion*

Corp., 541 P.2d 663, 664–65 (Nev. 1975). The formation of an enforceable contract requires the following: (1) offer and acceptance, (2) meeting of the minds, and (3) consideration. *May v. Anderson*, 119 P.3d 1254, 1257 (Nev. 2005). As stated above, the damages element has been sufficiently pled. *See supra*.

The Houghton plaintiffs allege that they formed an implied contract with Eureka and that by not implementing sufficient security measures, Eureka breached that contract. ECF No. 31 at ¶¶ 159–78. They claim that by providing their PII in exchange for Eureka's services and products, Eureka impliedly agreed to reasonably protect the information. *Id.* at 35. The Houghton plaintiffs also allege that they "expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards" and those "who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security." *Id.* According to the consolidated complaint, the Houghton plaintiffs

> would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

Id. at 36. In its motion, Eureka argues that (1) no implied contract was formed, (2) the plaintiffs failed to allege that any breach occurred, and (3) there was no consideration. ECF No. 41 at 14–18. Although the Houghton plaintiffs address the issues of contract formation and breach in their response, they fail to address Eureka's argument that no consideration existed in their purported implied contract. By not responding to this argument, the plaintiffs effectively conceded the validity of Eureka's motion on these grounds. Local Rule 7-2(d) provides, in relevant part, that "[t]he failure of a moving party to file points and authorities in support of the motion constitutes a consent to the denial of the motion." LR 7-2(d); *see also Travelers Cas. Ins. Co. of Am. v. Geragos & Geragos*, 495 F. Supp. 3d 848, 854 (C.D. Cal. 2020) ("Arguments to which no

response is supplied are deemed conceded."). Therefore, the Houghton plaintiffs' breach of implied contract claim is dismissed. But because the Houghton plaintiffs may be able to cure this deficiency, it is dismissed without prejudice and with leave to amend.

D. Unjust enrichment

The consolidated complaint alleges that the Houghton plaintiffs conferred a monetary benefit on Eureka when they made payments and provided Eureka with their personal information. ECF No. 31 at ¶ 191. They allege that their reasonable expectation was that Eureka would use part of the money to protect their information, but Eureka "instead calculated to increase their own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures." *Id.* They seek Eureka's disgorgement of all proceeds Eureka "unjustly received" from the plaintiffs. *Id.* at ¶ 198.

Eureka argues that the Houghton plaintiffs' unjust enrichment claim fails for three reasons. ECF No. 41 at 18–19. It argues that the plaintiffs cannot sufficiently allege facts to satisfy the elements of the claim because "[t]here is nothing unjust about a casino and hotel receiving a customer's personal information to: (1) provide gambling, lodging and hospitality services; (2) comply with tax laws regarding gambling winnings; or (3) offer the customer other benefits of being a players rewards club member." *Id.* (citing *In re SuperValu, Inc.*, 925 F.3d 955, 966 (8th Cir. 2019)). It argues that, because the plaintiffs do not seek the return of their PII, "or compensation for any monetary value they could ascribe to such[,]" they do not allege compensable damages. *Id.* at 19. Finally, Eureka argues that the plaintiffs fail to explain why monetary damages would be inadequate. *Id.* at 18. The Houghton plaintiffs respond that they paid Eureka for its services expecting that part of their payments would go to reasonable security measures for their PII, and Eureka's failure to do so amounted to unjust enrichment. ECF No. 42 at 21–22. They also argue that the compensable damages are "the portion of payments made by Plaintiffs to Eureka to provide reasonably [sic] data security measures, but which Eureka nevertheless failed to

implement—not Plaintiffs' Personal Information provided to Eureka nor the value of such information." *Id.* at 22. They also insist they cannot be remedied by money damages alone. *Id.*

In Nevada, the elements of an unjust enrichment claim are: "(1) a benefit conferred on the defendant by the plaintiff; (2) appreciation of the benefit by the defendant; and (3) acceptance and retention of the benefit by the defendant; (4) in circumstances where it would be inequitable to retain the benefit without payment." *Ames v. Caesars Ent. Corp.*, 2019 WL 1441613, at *5 (D. Nev. Apr. 1, 2019) (quoting *Leasepartners Corp. v. Robert L. Brooks Tr.*, 942 P.2d 182, 187 (Nev. 1997)). Unjust enrichment and disgorgement are equitable remedies. *See Small v. Univ. Med. Ctr. of S. Nev.*, 2016 WL 4157309, at *3 (D. Nev. Aug. 3, 2016) ("Nevada recognizes the general rule that an equitable claim, like unjust enrichment, is not available where the plaintiff has a full and adequate remedy at law."); *Sunlighten, Inc. v. Finnmark Designs, LLC*, 595 F. Supp. 3d 957, 972 (D. Nev. 2022) ("Disgorgement is an equitable remedy[.]"). Thus, for a plaintiff to succeed in an unjust enrichment claim, they must show that they lack an adequate remedy at law. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844–45 (9th Cir. 2020).

Here, payment alone is sufficient to establish that a benefit was conferred on the defendant. *See Certified Fire Prot. Inc. v. Precision Constr.*, 283 P.3d 250, 257 (Nev. 2012) ("Benefit in the unjust enrichment context can include services beneficial to or at the request of the other, denotes any form of advantage, and is not confined to retention of money or property." (internal quotations omitted)). Not only did the Houghton plaintiffs pay Eureka, but they also allege that part of their payment was to be used for protection of their data. ECF No. 31 at ¶ 191. Eureka likewise appreciated, accepted, and retained the benefit because it accepted the plaintiffs' payment. The remaining question is whether this occurred in "circumstances where it would be inequitable to retain the benefit without payment." *Ames*, 2019 WL 1441613, at *5. The Houghton plaintiffs advance two separate theories: first, that they overpaid for the services assuming that Eureka would provide adequate data protection; and second, that, had they known that Eureka's systems were allegedly not compliant with industry standards, they would not have

paid for Eureka's service in the first place. *See* ECF No. 31 at ¶¶ 191–94. The plaintiffs' first theory is subject to a split of authority. *Compare Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012), *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1201 (D. Or. 2016), *and In re Banner Health Data Breach Litig.*, 2017 WL 6763548, at *6 (D. Ariz. Dec. 20, 2017) (data breach cases finding that the overpayment theory of unjust enrichment overcomes a motion to dismiss), *with Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016), *and Carlsen v. GameStop, Inc.*, 833 F.3d 903, 912 (8th Cir. 2016) (finding that it does not).

Here, I find that the plaintiffs have alleged enough to survive the motion to dismiss on their unjust enrichment claim based on their first theory.[9] Eureka's argument that there is nothing unjust about a casino seeking payment for services neglects the crux of the plaintiffs' argument. A business can certainly expect payment in receipt for its products and services, but when part of that payment was made in exchange for protection of private information, as the plaintiffs allege here, a business has been unjustly enriched if it fails to erect those protections. Eureka also misconstrues the compensable damages the plaintiffs seek: it is not the return of the PII, it is the amount the Houghton plaintiffs paid that was intended to go to constructing adequate data protection measures.

Eureka also suggests that the plaintiffs do not sufficiently explain why damages are inadequate. ECF No. 41 at 18; ECF No. 43 at 9 (citing *Sonner*, 971 F.3d at 841, *Gardiner*, 2021 WL 4992539, at *7, and *Smallman*, 638 F. Supp. 3d at 1197). Like with many issues in the data breach context, there is some competing authority. *See, e.g.*, *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1086 (N.D. Cal. 2023) ("Meta also argues that the claim cannot stand as plaintiffs have failed to plead that they lack adequate remedies at law under *Sonner* . . . . But plaintiffs do allege that their remedies at law are inadequate.") Even in *Smallman*, the court noted that part of its

[9] The alternative theory, that the plaintiffs would not have used Eureka's services had they known about its allegedly deficient security, is not as well developed in the case law, but has found some support as well. *See, e.g.*, *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014). Because I find enough support under the plaintiffs' first theory, I do not reach a conclusion on the second theory.

reasoning for dismissing the plaintiffs' unjust enrichment claim was that "Plaintiffs have not alleged, even in the alternative, that they do not have adequate legal remedies." 638 F. Supp. 3d at 1198. I find that the allegation that legal remedies are inadequate is sufficient to survive a motion to dismiss. Therefore, Eureka's motion to dismiss the plaintiffs' unjust enrichment claim is denied.

E. UCL claim

The consolidated complaint alleges that Eureka violated California's UCL. ECF No. 31 at ¶¶ 199–213. The California UCL prohibits "unfair competition" and defines the term as a "business act or practice" that is (1) "fraudulent," (2) "unlawful," or (3) "unfair." Bus. & Prof. Code § 17200. Each prong of the UCL provides "a separate and distinct theory of liability[.]" *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1127 (9th Cir. 2009). To have standing to pursue a UCL claim, the Houghton plaintiffs must show that they "suffered injury in fact and ha[ve] lost money or property as a result of [Eureka's] unfair competition." Cal. Bus. & Prof. Code § 17204. *See also In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 804 (N.D. Cal. 2019). In its motion, Eureka argues that the Houghton plaintiffs have not alleged they suffered an injury in fact to establish standing, that they do not state their claim with sufficient specificity under the "fraudulent" prong, and that their claims likewise fail under the "unlawful" and "unfair" prongs. ECF No. 41 at 19–20; ECF No. 43 at 9–10.

1. Standing

Eureka argues that, because the Houghton plaintiffs allege only that their PII "is of tangible value[,]" and do not state they suffered identity theft or fraudulent charges, they do not have standing to bring a UCL claim. ECF No. 41 at 20–21. However, as discussed previously, the plaintiffs repeatedly allege that a part of their payment to Eureka was designed to ensure adequate safety measures, which were allegedly not provided. *See* ECF No. 31 at ¶¶ 191–94. This is sufficient to establish an injury in fact. *See Smallman*, 638 F. Supp. 3d at 1201–02 (finding that plaintiffs sufficiently pled allegations establishing standing where plaintiffs alleged that they

paid the "overinflated cost of the hotel rooms they purchased as a result of Defendant['s] omissions regarding the adequacy of data security policies.")

2. Fraudulent and unlawful prongs

When alleging fraud, plaintiffs must meet a heightened pleading standard that requires they "state with particularity the circumstances constituting fraud including the who, what, when, where and how of the misconduct charged." *Loomis v. U.S. Bank Home Mortg.*, 912 F. Supp. 2d 848, 856 (D. Ariz. 2012) (quoting Fed. R. Civ. P. 9(b)). In their opposition, the plaintiffs argue that their claim falls only under the "unlawful" and "unfair" prongs and thus does not require the heightened fraud pleading. ECF No. 42 at 23. Eureka's reply argues that the plaintiffs' claims are "attempted obfuscation" and because they state that Eureka violated Section 5(a) of the FTC Act—a predicate for their "unlawful" prong claim— "by misrepresenting, by omission, the safety of their computer systems," their claim should actually be viewed under the "fraudulent" prong.

The "unlawful" prong of the UCL "borrows violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable." *Cal. Consumer Health Care Council v. Kaiser Found. Health Plan, Inc.*, 142 Cal. App. 4th 21, 27 (2006) (internal quotations omitted). Thus, in determining whether the "unlawful" prong has been met, the court must "look through" the asserted UCL claim and determine if the underlying statutes cited state a claim for relief. *Id.* at 28. As discussed above, the plaintiffs' "unlawful" prong argument is based on Eureka's alleged violation of Section 5(a) of the FTC Act. ECF No. 42 at 23–24.

Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." 15 U.S.C. § 45(a)(1). A plaintiff can rely on this statute to make an "unlawful" prong claim; fraud is not a necessary element, and the plaintiffs do not attempt to make a case for fraud. *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 992, 995 (N.D. Cal. 2016) [(*Anthem II*)]; *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 420 (E.D. Va. 2020) ("Section 5 of the FTC Act applies here and provides an

ascertainable duty regarding data protection. . . . Therefore, Plaintiffs have adequately alleged the unlawfulness prong of an UCL claim.").

The Houghton plaintiffs allege that Section 5 of the FTC Act creates an independent statutory duty for businesses to "implement basic data security practices" and that orders from the FTC's enforcement actions "further clarify the measures businesses must take to meet their data security obligations." ECF No. 31 at ¶¶ 55–56. They also argue that Eureka violated Section 5(a) by "failing to implement reasonable and appropriate security measures or follow industry standards for data security, by failing to ensure its affiliates with which it directly or indirectly shared the PII did the same, and by failing to timely notify Plaintiff Houghton's and California Subclass Members of the Data Breach." *Id.* at ¶ 205. Houghton alleges that if Eureka had complied with Section 5(a), he and Class Members would not have been damaged. *Id.* at ¶ 206. These allegations are sufficient to establish a claim under the "unlawful" prong, so I deny Eureka's motion to dismiss the Houghton plaintiffs' UCL claim under the "unlawful" prong.

3. Unfair prong

Eureka also argues that the Houghton plaintiffs' conclusory assertion that it failed to implement and maintain reasonable data security measures is insufficient to satisfy the "unfair" prong of the UCL. ECF No. 43 at 10. The "unfair" prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *23 (N.D. Cal. Aug. 30, 2017) (citing *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143 (2003)).

"The UCL does not define the term 'unfair' . . . [and] the proper definition of 'unfair' conduct against consumers 'is currently in flux' among California courts." *Id.* However, to determine whether something is "unfair," many California courts will "weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim." *Davis v. HSBC Bank*

Nevada, N.A., 691 F.3d 1152, 1169 (9th Cir. 2012) (internal quotation marks omitted).[10] Under this approach, the Houghton plaintiffs "may proceed with a UCL claim under the balancing test by either alleging immoral, unethical, oppressive, unscrupulous or substantially injurious conduct by [Eureka] or by demonstrating that [Eureka's] conduct violated an established public policy." *Anthem II*, 162 F. Supp. 3d at 990.

The plaintiffs here allege that Eureka's knowing failure to ensure adequate safeguards of their PII violated several California statutes, including Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). ECF No. 31 at ¶ 210. District courts in this circuit, presented with similar allegations have consistently found that plaintiffs have alleged enough for the "unfair" prong to be resolved at a later stage of litigation. *See In re Yahoo!*, 2017 WL 3727318, at *24 (collecting cases). On one side of the balancing test, I must weigh the utility of the defendant's conduct as alleged: there is little utility in Eureka's failing to follow data security laws. On the other, the harm to the plaintiffs of having their PII stolen is potentially far greater. As a result, I find that the Houghton plaintiffs have sufficiently alleged a claim, so I deny Eureka's motion to dismiss the plaintiffs' UCL claim under the "unfair" prong.

[10] There are several other formulations of this test, including the "tethering test" and the "FTC test," but courts have found that a plaintiff's ability to allege the defendants' violation of the balancing test has, alone, been sufficient to survive a motion to dismiss. *See, e.g.*, *In re Yahoo!*, 2017 WL 3727318, at *23–24.

F. CCPA claim

The Houghton plaintiffs allege that Eureka violated the CCPA. ECF No. 31 at ¶¶ 214–28. The CCPA permits "[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action." Cal. Civ. Code § 1798.150(a)(1).

Eureka first argues that the Houghton plaintiffs make conclusory allegations that fail to state a plausible CCPA claim. ECF No. 41 at 21. It specifically states that the plaintiffs rely entirely on the assertion that "[t]he Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect" the plaintiffs' PII. *Id.* (quoting ECF No. 31 at ¶¶ 217–18, 223). This, Eureka argues, is conclusory and does not meet the pleading standard required for a CCPA claim. *Id.* (citing *Iqbal*, 556 U.S. at 678; *In re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *6 (S.D.N.Y. Feb. 24, 2022); and others).

However, I find that the plaintiffs allege more than just conclusory statements. Looking at their consolidated complaint in its entirety, which was incorporated into their CCPA claims (ECF No. 31 at ¶ 214), the plaintiffs allege that Eureka (1) failed to encrypt the plaintiffs' PII (ECF No. 31 at ¶ 38); (2) failed to adhere to FTC guidelines, including not maintaining PII longer than needed, limiting access to PII, requiring complex passwords, failing to use industry tested methods of security, failing to monitor for suspicious activity and to verify that third-party providers implemented adequate security (ECF No. 31 at ¶¶ 54, 56); (3) failed to follow industry standards, including failing to install malware detection software, failing to set up network firewalls, and failing to follow the Center for Internet Security's Critical Security Controls (ECF No. 31 at ¶¶ 59–61); and:

> a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
> b. Failing to adequately protect customers' Private Information;
> c. Failing to properly monitor its own data security systems for existing intrusions, encryptions, brute-force attempts, and clearing of event logs;
> d. Failing to apply all available security updates;
> e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;
> f. Failing to practice the principle of least-privilege and maintain credential hygiene;
> g. Failing to avoid the use of domain-wide, admin-level service accounts;
> h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;
> i. Failing to properly train and supervise employees in the proper handling of inbound emails.

(ECF No. 31 at ¶ 62). Additionally, the Houghton plaintiffs allege that "Eureka admitted it had failed to maintain security appropriate to the nature of the information when it stated that it only 'took steps to secure our system' after the Data Breach occurred." ECF No. 42 at 27 (citing ECF No 31 at ¶ 39).

These allegations are more than sufficient to plausibly plead a violation of the CCPA. At this stage of litigation, with discovery incomplete, it would be unrealistic to expect a plaintiff to provide more detail about the defendant's former security systems. *See Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1220 (11th Cir. 2023).

Next, Eureka argues that the plaintiffs' claims are barred under the language of the CCPA. The CCPA allows plaintiffs to seek relief for "actual pecuniary damages," for statutory damages, or for both. Cal. Civ. Code § 1798.150(b). Eureka states that the plaintiffs are only

seeking statutory damages,[11] and they failed to comply with the pre-suit statutory damages notice requirement. Under the CCPA:

> Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.

Cal. Civ. Code § 1798.150(b). Eureka argues that the plaintiffs provided untimely pre-suit notice of their statutory claims, barring their statutory claim. ECF No. 41 at 22–23. It states that Houghton originally filed his individual complaint on February 22, 2023, and mailed the CCPA pre-suit notice the same day. *Id.* (citing ECF No. 1 and ECF No. 31 at ¶ 224). Houghton's complaint contained no mention of the CCPA. *See* ECF No. 1. Only when the consolidated complaint was filed, on June 16, 2023, did plaintiffs raise a statutory damages CCPA claim. ECF No. 31 at ¶ 214. In support of its argument that the claim is barred for lack of notice, Eureka relies on *Griffey v. Magellan Health Inc.*, in which the court declared that "[i]f a notice filed before the 30-day deadline could be updated when an amended complaint is filed and satisfy the 30-day notice requirement, then having the pre-suit notice requirement would be pointless." 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022). The court then dismissed the plaintiffs' CCPA claims with prejudice. *Id.*

I find the *Griffey* court's reasoning unpersuasive in this context. The CCPA's notice requirement is designed "to allow the defendant an opportunity to cure the defect outside of court." *Id.* (quoting *T & M Solar & Air Conditioning, Inc. v. Lennox Int'l Inc.*, 83 F. Supp. 3d 855, 875 (N.D. Cal. 2015)). There is no reason why the addition of a CCPA statutory damages claim to an

[11] Based on the consolidated complaint, the plaintiffs seek "statutory damages . . . or actual damages." ECF No. 31 at ¶ 228.

amended complaint, after thirty days' notice has been given, would go against the intentions of this law. It is one thing for a plaintiff to initially file a complaint seeking CCPA statutory damages in violation of the thirty-day notice requirement, only to file an amended complaint with the same claim thirty days later. There is no harm, however, to a defendant who (1) has been notified of a lawsuit on other grounds and (2) is separately provided thirty days' notice of the plaintiff's seeking statutory damages in a CCPA claim. If, thirty days later, the plaintiff determines that the defendant has not sufficiently cured its alleged violations, there should be no reason the plaintiff is prevented from pursuing those claims. The defendant was provided the statutorily mandated opportunity to cure before the plaintiff ever took the claim to court. Therefore, the plaintiffs complied with the CCPA statutory damages notice rule when they added the CCPA claim nearly four months after the notice letter was sent.

Eureka next argues that Houghton's February 22, 2023 notice letter was deficient because it did not "identify[] the specific provisions of [the CCPA] the consumer alleges have been or are being violated." ECF No. 41 at 23 (quoting Cal. Civ. Code § 1798.150(b)). It argues that the two provisions Houghton cited—California Civil Code §§ 1798.81.5 and 1798.150—are inadequate because § 1798.150 imposes no affirmative duty on the defendant and Houghton only made conclusory statements in support of § 1798.81.5. *Id.* Section 1798.81.5 requires a covered business to "implement and maintain reasonable security procedures and practices . . . ." Cal. Civ. Code § 1798.81.5.

I disagree. Nothing in the law suggests this notice is required to meet the same standards for pleading as a complaint. In the notice letter, Houghton explained that Eureka violated § 1798.81.5 by "fail[ing] to meet its duty to implement and maintain reasonable security procedures and practices . . . includ[ing] the lack of adequate encryption to sufficiently maintain California residents' PII and to protect this PII from being accessed by third parties without authorization." Notice letter, ECF No. 31-1 at 2. As discussed above, it would be unreasonable to expect a prospective plaintiff following a data breach, who has not been made privy to the inner

workings of Eureka's data encryption systems, to provide notice in great detail. I find this language to be sufficient under the notice requirement of the CCPA.

Finally, Eureka argues that it cured the issues noticed in Houghton's letter because, as it explained in its letter responding Houghton's notice letter,

> [u]pon learning of suspicious activity on its network, Rancho Mesquite immediately took measures to contain the incident, notified law enforcement, and began an investigation. Rancho Mesquite took the necessary steps to block the unauthorized access and has continued to monitor for any further suspicious activity or attempted or actual access to its network. None has been detected.

Eureka's notice letter response, ECF No. 31-2 at 3. However, "[t]he implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach." Cal. Civ. Code § 1798.150(b). Eureka's measures were designed for the purpose of addressing future threats, not curing the unauthorized release of the plaintiffs' data. Therefore, I deny Eureka's motion to dismiss the plaintiffs' CCPA claim.

G. CCRA claim

The Houghton plaintiffs allege that Eureka violated the CCRA. ECF No. 31 at ¶¶ 229–36. Under the CCRA, any business which "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b). Eureka argues that the plaintiffs make only a conclusory statement that "Defendant failed to maintain reasonable data security procedures appropriate to the nature of the personal information" and provide no additional factual allegations in support. ECF No. 41 at 24 (quoting ECF No. 31 at ¶ 234). However, the Houghton plaintiffs allege not only that their data was kept unsecure and unencrypted, which they describe in some detail, they also allege that Eureka delayed notice of the breach to many of its customers for months—further exposing its customers to harm. ECF No. 31 at ¶¶ 233, 36–37. I find that the plaintiffs have pled a CCRA

violation with sufficient specificity to overcome Eureka's motion, and therefore, I deny Eureka's motion to dismiss the plaintiffs' CCRA claim.

H. Declaratory judgment

Eureka's argument for dismissal of the Houghton plaintiffs' request for declaratory relief is contingent on the plaintiffs' negligence and implied contract claims having been dismissed. Because the negligence claim remains, I deny Eureka's motion to dismiss the plaintiffs' request for declaratory judgment.

IV. Conclusion

It is therefore ordered that Eureka's motion to dismiss **[ECF No. 41] is granted in part and denied in part.** The individual claims are addressed as follows:

(1) Eureka's motion as to the Houghton plaintiffs' negligence claim is **denied**.

(2) Eureka's motion as to the Houghton plaintiffs' negligence per se claim is **granted** and the negligence per se claim is therefore **dismissed without prejudice**.

(3) Eureka's claim as to the Houghton plaintiffs' breach of implied contract claim is **granted** and the implied contract claim is therefore **dismissed without prejudice**.

(4) Eureka's motion as to the Houghton plaintiffs' unjust enrichment claim is **denied**.

(5) Eureka's motion as to the Houghton plaintiffs' UCL claim is **denied**.

(6) Eureka's motion as to the Houghton plaintiffs' CCPA claim is **denied**.

(7) Eureka's motion as to the Houghton plaintiffs' CCRA claim is **denied**.

(8) Eureka's motion as to the Houghton plaintiffs' declaratory judgment claim is **denied**.

If plaintiffs intend on filing an amended complaint, it must be titled "Second Amended Complaint," and it must be filed on or before October 3, 2024.

Dated: September 19, 2024

Cristina D. Silva
United States District Judge